

Attachment A4

WVDirect Subscription Agreement

Overview

WVDirect is a service of the WV Health Information Network (WVHIN) created to promote the adoption and use of Direct Messaging for the secure and trusted transmission of patients' protected health information ("PHI"). All organizations and individuals participating in WVDirect's trusted healthcare community will be verified by a representative of the WVHIN or a Notary Public. The entity verification process allows WVDirect participants to be assured that other participants are actual members of the West Virginia healthcare community with a legitimate reason to send and receive PHI. In order to expand secure communications across WV's borders, WVDirect will establish connections with other providers of secure trusted Direct Messaging services.

In order to ensure the success and optimal utilization of WVDirect, it is important that all member entities:

- cooperate with each other,
- follow security best practices,
- provide accurate information,
- promptly update information when circumstances change,
- diligently monitor WVDirect accounts for incoming referrals, information, and requests, and
- respond to requests in a timely manner

Member Organization Information:

Organization Name	
Address 1	
Address 2	
City	
County	
State	
Zip Code	
Phone Number	
E-Mail Address	
Group NPI Number	
Fax Number (asso w/NPI)	
Point of Contact Name	
Business Web Address	

Required Documentation:

- Current copy of your business license
- Current copy of your professional licenses (for individual accounts)

Terms and Conditions

By signing below, your healthcare organization, its officers, directors and employees, agree to the following terms and conditions:

1. All information provided on this form is true and accurate as of the date of execution. Business and professional licenses must be kept current in order to remain WVDirect trusted healthcare subscribers.
2. If any of the information above changes, WVHIN will be notified as soon as possible via e-mail to direct@wvhin.org or phone 304-558-4503.
3. WVDirect accounts may be established for your organization as a whole and/or for individual employees. WVDirect accounts for individual employees may only be established for individual employees of your organization authorized to access, use, or transmit PHI in order to perform their job duties.
4. Access to WVDirect accounts established at the organizational level must be tightly controlled and monitored. Your organization must identify the Authorized Administrator responsible for controlling access to the organization's accounts.
5. Each individual shall be responsible for all activities associated with the account assigned to him or her.
6. Your organization must delete access to WVDirect accounts established for individual employees no longer employed by your organization within one (1) business day of the employee's last day at your organization. If an employee is terminated due to less than favorable circumstances, access to the account must be deleted immediately.
7. WVDirect accounts are to be used for the exchange of PHI between known and trusted WVDirect subscribers or with Direct subscribers of other health information service providers with which the WVHIN has entered into trusted contractual arrangements for the provision of health care on behalf of a Patient. WVDirect Subscribers may be health care providers, health plans, public health agencies, subscribers of other health information service providers, or other organizations that are involved in health care related activities and agree to comply with all the provisions of this Agreement. WVDirect accounts must not be used for any other purpose, including but not limited to, unauthorized commercial purposes, e-mail spamming, or marketing.
8. Your organization will encourage best practices for patient privacy protections related to the use of each WVDirect account associated with your organization, including those accounts established for individuals. In doing so, your organization will vigorously enforce the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") Privacy and Security Rules, including, with limitation, maintaining the confidentiality and security of PHI;

implementation of administrative, technical, and physical safeguards to prevent unauthorized access, use, and transmission of PHI; only access, use or disclose PHI as authorized by the patient; mitigate any risks associated with an unauthorized access, use, or disclosure of PHI; require any subcontractors that receive, use, or have access to PHI to comply with the Privacy and Security Rules; and disclose only the minimum PHI necessary for the purpose for which it is disclosed.

9. In connection with HIPAA and HITECH enforcement measures, your organization will strive to minimize the risk of participation in the WVDirect trusted healthcare community for other subscribers by carefully monitoring use of your computers and the WVDirect accounts to prevent transmitting programs or data (such as malware, viruses, worms, and Trojan Horses) which may impair operability or affect patient privacy rights or breach PHI security.
10. Your organization will conform to Security Best Practices. (Attachment A)
11. In accordance with WVHIN Policies, your organization will promptly notify WVHIN if there is a breach of the security of your system that may in any way affect your WVDirect accounts.
12. Your organization will execute a BAA with the WVHIN. (Attachment B). This Paragraph 12 is not applicable to state or federal public health agencies.
13. There will be no initial charge to participate in WVDirect. WVHIN reserves the right to begin charging a fee for use of the service upon 180 day written notice.
14. The WVHIN reserves the right to deny or remove access to WVDirect and the trusted healthcare community for any violation of the terms of this Agreement.

I hereby certify that my organization provides healthcare services to WV patients and I am authorized to act on behalf of the organization to participate in the WVDirect trusted healthcare community, to sign this Agreement and that the information contained herein is true and accurate.

Organization Name

WVHIN Representative

Corporate Officer Signature

Notary Public Signature (Note: A notary is not required if the signature has been verified by a WVHIN Representative)

Print Corporate Officer Name

Title

Date

Authorized Administrator Information

The Authorized Administrator is appointed to communicate with WVHIN and act on behalf of your organization with respect to all aspects of WVDirect. The Authorized Administrator is also responsible for maintaining the organization's individual WVDirect accounts, and for deleting those accounts in a timely manner consistent with this Agreement. The Authorized Administrator must provide valid government issued identification such as a current driver's license or passport in order to verify their identity.

Administrator Name	
Title	
Role	<input type="checkbox"/> Physician <input type="checkbox"/> NP/RN/MA <input type="checkbox"/> Administrator <input type="checkbox"/> Other _____
Govt Issued ID #	

Signature of Authorized Administrator: _____

Identity of Authorized Administrator verified by: _____

WVHIN Representative Signature _____

Notary Public Signature (Note: A notary is not required if the signature has been verified by a WVHIN representative)

Attachment A

West Virginia Health Information Exchange (WVHIN) WVDirect Security Best Practices

The following provide best practices on user-controlled activities related to the use of the WVDirect secure email service. These practices do not, in and of themselves, determine whether a WVDirect user is fully compliant with HIPAA Security and Privacy requirements as defined in “Security Standards for the Protection of Electronic Protected Health Information (EPHI)” (45 CFR Part 164, Subpart C), commonly known as the Security Rule, and in “Privacy of Individually Identifiable Health Information” (45 CFR Part 164, Subpart E), commonly known as the Privacy Rule.

Keep your computer secure:

When using WVDirect, it is important to follow the same security guidelines currently used at your practice for computers containing PHI. Because files containing PHI might need to be stored in your computer before they are attached to a Direct message, it is important that the computer is protected (i.e., whole-disk encryption, not left unattended and unlocked, etc.). It is also important to lockdown and encrypt your wireless network.

Download PHI from your WVDirect account only to a secured workstation computer:

WVDirect is a secure email application; however it should not to be accessed from non-secure devices such as public use workstations or home computers where security controls cannot be enforced. Public use workstations and other non-secure devices are those where general public access is allowed, or where security technical and physical security requirements cannot be applied and controlled. You should only download information from your WVDirect email account to a secured computer.

Accessing WVDirect via Mobile Devices

Accessing the WVDirect from mobile devices (laptops, smartphones, tablets, etc.) is not prohibited; however, each WVDirect subscriber organization and individual user should examine the risk associated with potentially having PHI located on these devices through the sharing of patient data. The following protection mechanisms should be implemented to protect any PHI shared through the WVDirect that is stored locally on a user device:

- Device password lock activated and used to gain local access to the given device,
- Virus and other malware protection, and
- File encryption and/or encryption of data at rest.

It is also strongly recommended that subscribing organizations include, but not be limited to, the following protection mechanisms for all devices used by their affiliated users:

- Establishing PHI deletion policies and media disposal procedures for mobile devices.
- Maintaining an accurate mobile device tracking and asset management program.
- Developing policies for the proper use or restriction of personal mobile devices for access to any PHI system.

Email Confidentiality Notices

Each WVDirect subscriber has a responsibility to ensure the protection of patient data that is viewed or discussed through WVDirect consistent with the HIPAA Privacy Rule, including disclosures to unauthorized individuals. Each WVDirect user must ensure that communications involving patient data are between authorized individuals and that any authorizations or consents required by applicable law are obtained prior to disclosure.

